

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

JEFFREY PACILLI, SAIMA MIAN,  
AMANDEEP SINGH, and MARILYN  
ROBLEDO, individually and on behalf  
of all others similarly situated,

Plaintiffs,

v.

CARRIER IQ, INC., AT&T INC., SPRINT  
NEXTEL CORPORATION, T-MOBILE  
USA, INC., HTC AMERICA, INC.,  
APPLE, INC., SAMSUNG  
ELECTRONICS AMERICA, INC.,  
SAMSUNG TELECOMMUNICATIONS  
AMERICA, LLC, and MOTOROLA  
MOBILITY, INC.,

Defendants.

Civil Action No. \_\_\_\_\_

**Jury Demand**

**CLASS COMPLAINT FOR:**

1. Violation of Federal Wiretap Act,  
18 U.S.C. § 2511 AND
2. Violation of Stored Electronic Communication  
Act, 18 U.S.C. § 2701; AND
3. Violation of Federal Computer Fraud and Abuse  
Act, 18 U.S.C. § 1030

**CLASS ACTION COMPLAINT**

*“This is my worst nightmare . . . It is an utterly appalling invasion of privacy with immense potential for manipulation and privacy theft that requires immediate federal intervention.”*

Stephen Wicker, Cornell University Professor of Electrical and Computer Engineering, commenting on the Carrier IQ scandal

Plaintiffs Mr. Jeffrey Pacilli, Ms. Saima Mian, Mr. Amandeep Singh, and Ms. Marilyn Robledo (together, the “Plaintiffs”), on behalf of themselves and all others similarly situated, by and through their undersigned counsel, upon knowledge as to themselves and otherwise upon information and belief, allege as follows:

### NATURE OF THE ACTION

1. This is a class action lawsuit arising out the cell phone tracking scandal brought by, and on behalf of, similarly situated persons who had a wireless contract with at least one of the Defendant wireless phone carriers – AT&T Inc. (“AT&T”), Sprint Nextel Corporation (“Sprint”), or T-Mobile USA, Inc. (“T-Mobile”) – and who used at least one cell phone manufactured and/or distributed by at least one Defendant Manufacturer – Apple, Inc. (“Apple”), HTC America, Inc. (“HTC”), Samsung Telecommunications America, LLC or Samsung Electronics America, Inc. (together, “Samsung”) or Motorola Mobility, Inc. (“Motorola”) – which contained “rootkit” software designed and sold by Defendant Carrier IQ, Inc. (“Carrier IQ”) and whose privacy was violated.

2. Carrier IQ sells rootkit software designed to help wireless service providers and device makers identify and diagnose service and quality-related problems such as dropped calls and battery drain. The software is currently installed on 150 million phones worldwide.

3. Last month, Connecticut technology blogger Trevor Eckhart reported that the Carrier IQ software does more than advertised. The software is surreptitiously logging and transmitting extraordinarily sensitive information from consumers’ phones to the mobile phone carriers, without the knowledge or consent of the users, in violation of federal privacy laws.

4. On November 30, 2011, The United States Senate Committee on the Judiciary wrote a letter to Carrier IQ, expressing deep concern about the scandal. Demanding immediate responses to 11 questions, the letter says that the actions alleged “may violate federal privacy laws, including the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act. *This is a potentially very serious matter.*” (emphasis added).

5. Defendants’ willful and knowing actions violated the Federal Wiretap Act, the

Stored Electronic Communication Act, and the Federal Computer Fraud and Abuse Act. The Plaintiffs seek damages and injunctive relief under these statutes on behalf of the entire Class for these violations.

### **JURISDICTION AND VENUE**

6. This Court has personal jurisdiction over all Defendants because all conduct business in this District. In addition, Defendants AT&T, T-Mobile, Samsung and Motorola are incorporated under the laws of Delaware.

7. This Court has subject matter jurisdiction over this action and Defendants pursuant to 28 U.S.C. § 1331 because this action arises under federal statutes, namely the Federal Wiretap Act, 18 U.S.C. § 2511 (the “Wiretap Act”), the Stored Electronic Communication Act, 18 U.S.C. § 2701 (“SECA”) and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the “CAFA”) and pursuant to 28 U.S.C. § 1332(d) because the amount in controversy exceeds \$5,000,000.

8. Venue is proper in this District because all conduct business in this District. In addition, Defendants AT&T, T-Mobile, Samsung and Motorola are incorporated under the laws of Delaware.

### **THE PARTIES**

9. Plaintiff Jeffrey Pacilli is an adult domiciled in New Jersey. Mr. Pacilli is an AT&T customer and uses an Apple phone.

10. Plaintiff Saima Mian is an adult domiciled in New Jersey. Ms. Mian is a Sprint customer and uses an HTC phone.

11. Plaintiff Amandeep Singh is an adult domiciled in New Jersey. Mr. Singh is a T-Mobile customer and uses an Apple phone.

12. Plaintiff Marilyn Robledo is an adult domiciled in New Jersey. Ms. Robledo is an AT&T customer and uses a Samsung phone.

13. Defendant Carrier IQ is a California corporation based in Mountain View, CA. Carrier IQ designed the rootkit software at issue in this case.

14. Defendant AT&T is a Delaware corporation based in Dallas, TX.

15. Defendant T-Mobile is a Delaware corporation based in Bellevue, WA.

16. Defendant Sprint is a Kansas corporation based in Overland Park, KS.

17. Defendant Apple, Inc. is a California corporation based in Cupertino, CA.

18. Defendant HTC is a Texas corporation based in Bellevue, WA.

19. Defendant Samsung Electronics America, Inc. is a New York corporation base in Ridgefield Park, NJ.

20. Defendant Samsung Telecommunications America, LLC is a Delaware limited liability company based in Richardson, TX.

### **FACTUAL BACKGROUND**

21. Mountain View, California-based Carrier IQ sells software designed to help wireless service providers and device makers identify and diagnose service and quality-related problems such as dropped calls and battery drain. The software can be used to collect data for analyzing service quality and what Carrier IQ calls “mobile customer experience.”

22. The software is a type of rootkit software, which enables continued privileged access to a computer (including smart phones and other mobile phones) while actively hiding its presence from administrators by subverting standing operating functionality and other applications.

23. Carrier IQ claims to be the market leader in sales of “mobile service intelligence”

rootkit software.

24. Defendants Samsung, Apple, Motorola, and HTC pre-install Carrier IQ software on cell phones used by its customers on the AT&T, T-Mobile and Sprint networks.

25. Last month, a technology blogger and security researcher in Connecticut named Trevor Eckhart discovered that this Carrier IQ software was conducting surreptitious and highly intrusive tracking of cell phones. Eckhart described the software as a keystroke logging rootkit that is hard-to-detect, hard-to-remove and programmed to run by default on millions of handsets without the users' knowledge.

26. In addition to collecting device and service-related data, Carrier IQ's software can collect data about a user's location, application use, Web browsing habits, videos watched, texts read and even the keys they press.

27. The software runs when the phone is switched on and can log all activities until it is switched off.

28. AT&T and Sprint have already admitted that their handsets run Carrier IQ's software. HTC and Samsung confirmed that their phones include the software, but both told the press that it was only added after requests of the carriers.

29. The Electronic Privacy Information Center, a non-profit organization in Washington, D.C., noted that the use of Carrier IQ's software to log data may constitute an "unlawful intercept."

30. Former Unites States Department of Justice prosecutor Paul Ohm said that the use of the software could be grounds for private legal action.

31. On November 30, 2011, The United States Senate Committee on the Judiciary wrote a letter to Carrier IQ, expressing deep concern about the scandal. Demanding immediate

responses to 11 questions, the letter says that the actions alleged “may violate federal privacy laws, including the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act. *This is a potentially very serious matter.*” (emphasis added).

### **CLASS ACTION ALLEGATIONS**

32. This is a class action pursuant to Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure on behalf of a Class of all persons who had a wireless contract with at least one of the Defendant wireless phone carriers – AT&T, Sprint, or T-Mobile – and who used at least one cell phone manufactured and/or distributed by at least one Defendant Manufacturer – Apple, HTC Samsung or Motorola – which contained rootkit software designed and sold by Carrier IQ and whose privacy was violated. Excluded from the Class are the Court and any of the Court’s family members, Defendants, and their officers, directors, employees, affiliates, legal representatives, predecessors, successors and assigns, and any entity in which any of them have a controlling interest.

33. The members of the Class are so numerous that joinder of all members is impracticable.

34. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. The questions of law and fact common to the Class include whether Defendants violated the same federal laws.

35. Plaintiffs’ claims are typical of the claims of other Class members, as all members of the Class were similarly affected by Defendants’ wrongful conduct in violation of federal law as complained of herein.

36. Plaintiffs will fairly and adequately protect the interests of the members of the Class and have retained counsel that is competent and experienced in class action litigation.

Plaintiffs have no interest that is in conflict with, or otherwise antagonistic to the interests of the other Class members.

37. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in management of this action as a class action.

## **COUNT I**

### **VIOLATION OF THE FEDERAL WIRETAP ACT, 18 U.S.C. § 2511**

38. Plaintiffs incorporate the above allegations by reference as if set forth more fully herein.

39. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, prohibits the willful interception of any wire, oral, or electronic communication.

40. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

41. Defendants placed rootkit software on plaintiffs' phones that intercepted records of users' phone communications.

42. Neither the Plaintiffs nor members of the Class consented to or were aware that the Defendants were violating federal law and tracking this information.

43. The data that the Defendants knowingly intercepted are "communications" within the meaning of the Wiretap Act.

44. Defendants intentionally and willfully placed the software on users' phones and

handset devices and intentionally and willfully intercepted the electronic communications of such users.

45. Plaintiffs are persons whose electronic communications were intercepted within the meaning of Section 2520.

46. Section 2520 provides for preliminary, equitable and declaratory relief, in addition to statutory damages of the greater of \$10,000 or \$100 a day for each day of violation, actual and punitive damages, reasonable attorneys' fees, and disgorgement of any profits earned by Defendants as a result of the above-described violations.

## **COUNT II**

### **VIOLATION OF THE STORED ELECTRONIC COMMUNICATIONS ACT,**

#### **18 U.S.C. § 2701**

47. Plaintiffs incorporate the above allegations by reference as if set forth more fully herein.

48. The Stored Electronic Communications Act ("SECA") provides a cause of action against a person who intentionally accesses without authorization a facility through which an electronic communication service is provided, or who intentionally exceeds an authorization to access that facility, and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in storage in such a system.

49. "Electronic Storage" is defined in the statute to be "any temporary, immediate storage of a wire or electronic communication incidental to the electronic transmission thereof."

50. Defendants intentionally placed software on users' phones that accessed their stored electronic communications without authorization, and thus violated SECA.

51. Plaintiffs and other member of the Class were harmed by Defendants' violations,

and are entitled to statutory, actual and compensatory damages, injunctive relief, punitive damages, and reasonable attorneys' fees.

**COUNT III**

**VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT,**

**18 U.S.C. § 1030**

52. Plaintiffs incorporate the above allegations by reference as if set forth more fully herein.

53. Defendants intentionally accessed a computer used for interstate commerce or communication, without authorization or by exceeding authorized access to such a computer, and by obtaining information from such a protected computer.

54. Defendants knowingly caused the transmission of a program, information, code or command and as a result caused a loss to one or more persons during any one-year period of at least \$5,000 in the aggregate.

55. Plaintiffs have also suffered a violation of the right of privacy as a result of Defendants' knowing actions.

56. Defendants have thus violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

57. Plaintiffs' phones are "computers" within the meaning of the Act.

58. Defendants' unlawful access to Plaintiff's computers and communications have caused irreparable injury. Unless restrained and enjoined, Defendant may continue to commit such acts. If Plaintiffs' remedies at law are not adequate to compensate for these inflicted and threatened injuries, Plaintiffs and the Class are entitled to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs respectfully request that this Court:

A. Determine that this action is a proper class action under Rule 23 of the Federal Rules of Civil Procedure;

B. Award compensatory damages, including statutory damages where available, in favor of Plaintiffs and the other members of the Class against Defendants for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Permanently restrain Defendants, and its officers, agents, servants, employees and attorneys, from installing software on cell phones that could track the users' information in violation of federal law;

D. Award Plaintiffs and the Class their reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

E. Grant Plaintiffs such further relief as the Court deems appropriate.

**JURY TRIAL DEMAND**

The Plaintiffs demand a trial by jury of all issues so triable.

Respectfully submitted,

Dated: December 2, 2011.

